UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/057,066	01/25/2002	Sihai Xiao	TVW/APP35US	5026

59906 7590 01/12/2007

PATTERSON & SHERIDAN, LLP
TVWORKS, LLC
595 SHREWSBURY AVENUE
SUITE 100
SHREWSBURY, NJ 07702

EXAMINER	
PICH, PONNOREAY	
ART UNIT	**PAPER NUMBER**
2135	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/12/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/057,066	XIAO, SIHAI	
	Examiner	Art Unit	
	Ponnoreay Pich	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 October 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22,24-46,48 and 49* is/are pending in the application.

4a) Of the above claim(s) *7-13 and 31-37* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,14-22,24-30,38-46,48 and 49* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10/25/2006 has been entered. Any well known art statements made in the prior office action not specifically and/or adequately traversed by applicant are taken as admittance of prior art as per MPEP 2144.03.

Claims 1-22, 24-46, and 48-49 are pending. Claims 7-13 and 31-37 are withdrawn from consideration as per a prior election by applicant. Applicant's amendments were fully considered. Applicant's arguments with regards to the amended claims were also fully considered, but are moot in view of new rejections presented below.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-2, 22, 24-26, and 46 are rejected under 35 U.S.C. 102(e) as anticipated by or, in the alternative, under 35 U.S.C. 103(a) as obvious over Hericourt et al (US 2002/0078347).

Claims 1 and 46:

Hericourt discloses:

1. Providing/receiving a trust information object (TIO) to/at said client (paragraphs 100, 107, and 175), wherein said TIO comprises associated trust information indicating a level of trust for a trusted entity associated with said trust entity certificate (paragraph 175), wherein the trusted entity comprises a certificate authority (paragraphs 147-152); and
2. Verifying a received certificate using at least a portion of said TIO (paragraphs 104).

The examiner is considering the response from CA Filter 309 which comprises at least a CA trust level and a certificate of the CA to be a TIO. Hericourt does not *explicitly* disclose said TIO as disclosed in his invention also comprises a hash value of

a trust entity certificate. However, Hericourt discusses in paragraphs 11-17 that an X.509 certificate's formal structure includes a signature of the certificate, i.e. a hash value of the certificate. Note that Hericourt does not place any restrictions on the types of certificates used in his invention. In discussing X.509 certificates in his background section, it would not have been beyond the scope of Hericourt's invention where the certificate used included X.509 certificates. When these certificates are returned in the response from a CA Filter, a hash value of the CA's certificate is also returned. Thus, if interpreted broadly, Hericourt can be considered 102 art as Hericourt does not place any restrictions on the types of certificates used in his invention and he discloses knowing about certificates that contained that hash value of a trust entity certificate. Since the TIO includes the trust entity certificate, the TIO, i.e. response from the CA Filter, can implicitly comprise a hash value of a trust entity certificate.

Alternatively, the limitations recited in claims 1 and 46 are also rendered obvious over Hericourt's teachings in light of what is discussed above. It would have been obvious to one of ordinary skill in the art to utilize an X.509 certificate within Hericourt's invention, such that the TIO also comprises a hash value of a trust entity certificate. One skilled would have been motivated to do so because X.509 is a standard for public key infrastructures.

Claim 2:

Hericourt further discloses wherein said TIO comprises any of the following: a trusted entity's certificate; a trust vector of said trusted entity's certificate; a value indicating a number of signatures required for a next update; a date said TIO is created;

and a digital signature of all data including said certificate, trust vector, number of signatures, and time stamp, contained in said TIO (paragraphs 100, 107, and 175).

Claim 48:

Hericourt further discloses wherein said TIO comprises any of: a time stamp which indicates a data that said TIO is generated; a trust attribute that comprises trust information associated with an entity represented by its certificate; and a thump print comprising a hash of a public key embedded in a certificate that represents a trusted entity (paragraphs 100, 107, and 175).

Claims 22 and 25:

Claims 22 and 25 are directed towards an apparatus comprising a client device which performs the method of claim 46, said client device comprising memory for storing said TIO as recited in claim 46. Note Hericourt discloses a client which performs the method of claim 46 (Fig 3, item 302). The client is disclosed as capable of storing TIO data (paragraph 107), thus has memory. As such, claims 22 and 25 are rejected for much the same reasons given in claim 46. Claims 22 and 25 only differs in what is recited in the preamble, which is not given patentable weight as the body of both claims are able to stand alone from the intended use recited in the preamble.

Claim 24:

Hericourt further discloses said TIO comprising any of: a time stamp which indicates a date that said TIO is generated; a trust attribute, i.e. trust level information, that comprises trust information associated with an entity represented by its certificate;

and a thumb print comprising a hash of a public key embedded in a certificate that represents a trusted entity (paragraph 175).

Claim 26:

Hericourt further discloses wherein said TIO comprises any of: a trusted entity's certificate; a trust vector of said trusted entity's certificate; a value indicating a number of signatures required for a next update; a data said TIO is created; and a digital signature of all data including said certificate, trust vector, number of signatures and timestamp, contained in said TIO (paragraph 175).

Claims 3-4 and 27-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hericourt et al (US 2002/0078347) in view of Vogel et al (US 6,816,900).

Claims 3 and 27:

Hericourt does not explicitly disclose wherein said hash value is determined using any of MD5 and SHA-1. However, Vogel discloses wherein a hash value is determined using any of MD5 and SHA-1 (col 7, lines 45-63).

At the time applicant's invention was made, it would have been obvious to one skilled in the art to modify Hericourt's invention such that said hash value is determined using any of MD5 and SHA-1. One skilled would have been motivated to do so because both MD5 and SHA-1 are conventional ways of obtaining hash values for signatures.

Claims 4 and 28:

Hericourt does not explicitly disclose wherein said TIO conforms to the PKCS#7 standard. However, Vogel discloses the PKCS#7 standard being used to sign messages (col 7, lines 37-44). At the time applicant's invention was made, it would have been obvious to one skilled in the art to modify Hericourt's invention such that said TIO conforms to the PKCS#7 standard. One skilled would have been motivated to do so because PKCS#7 offers a high level of security and is the standard for signing messages using certificates under a PKI. Hericourt discloses messages signed via certificates (paragraph 76).

Claims 5 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hericourt et al (US 2002/0078347) in view of applicant's admittance of prior art, herein AAPA, and further in view of Vogel et al (US 6,816,900).

Claims 5 and 29:

Hericourt does not explicitly disclose hard coding a TIO derived from a set of root certificate authority (CA) certificates into said client's software/ software of said client device. However, AAPA discloses that at the time applicant's was made, it was a common approach in the art to hard code a TIO into a client's software (specification, page 2, lines 4-6). Further, the examiner asserts that it was well known to derive a TIO from a set of root CA certificates. This is further evidenced by Vogel (col 4, lines 5-37).

At the time applicant's invention was made, it would have been obvious to one of ordinary skill to further modify Hericourt's invention by hard coding a TIO derived from a

set of root CA certificates into said client's software. One of ordinary skill would have been motivated to hard code a TIO into a client's software because as applicant discloses in the specification, it was a common approach in the art to provide associated trust information (specification, p2, lines 4-6). One skilled would have been motivated to derive a TIO from a set of root CA certificates because it would offer a high level of security for the certificate in the TIO since the certificate would be verified by a chain of CA's.

Claims 6, 30, and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hericourt et al (US 2002/0078347).

Claims 6 and 30:

Hericourt does not explicitly disclose saving a copy of said TIO in a persistent memory during said client's build time. However, as discussed in prior office action(s), it was well known in the art to save a copy of a TIO in a persistent memory during said client's build time, i.e. certificates, passwords, or keys are often assigned to a client when the client is built and saved in static memory to prevent the information from being lost when the client loses power.

At the time applicant's invention was made, it would have been obvious to further modify Hericourt's invention such that a copy of the TIO was saved in a persistent memory during said client's build time. One of ordinary skill would have been motivated to do so because it was common to assign trust information to a client during build time

and to save it in persistent memory to prevent lost of the information due to power failure.

Claim 49:

Hericourt discloses:

1. Providing a trust information object (TIO) to said client (paragraphs 100, 107, and 175), wherein said TIO comprises associated trust information indicating a level of trust for a trusted entity associated with said trust entity certificate (paragraph 175), wherein the trusted entity comprises a certificate authority (paragraphs 147-152); and
2. Verifying a received certificate using at least a portion of said TIO (paragraphs 104).

The examiner is considering the response from CA Filter 309 which comprises at least a CA trust level and a certificate of the CA to be a TIO. Hericourt does not explicitly disclose said TIO also comprise a hash value of a public key embedded in a certificate that represents a trusted entity. However, note that Hericourt does not place any restrictions on the type of certificates used in his invention. The examiner take official notice that certificates with a hash value of a public key embedded in the certificate that represents a trusted entity, i.e. CA, was well known in the art at the time applicant's invention was made. It would have been obvious to one skilled in the art to modify Hericourt's invention according to the limitations recited in claim 49. One skilled would have been motivated to do so because embedding the hash value of a public key

embedded in the certificate would provide a way to identify which public key to use to authenticate the certificate.

Claims 14-17, 20-21, 38-41, and 44-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hericourt et al (US 2002/0078347) in view of Samar (US 6,304,974).

Claim 14:

Hericourt discloses embedding a trust information object (TIO) within a client (paragraphs 100, 107, and 175), said TIO comprising associated trust information indicating a trust level for a trusted entity associated with said trust entity certificate (paragraph 175), wherein the trusted entity comprises a certificate authority (paragraphs 147-152).

Hericourt does not explicitly disclose said TIO of his invention also comprising a hash value of a trust entity certificate. However, for the reasons given in claims 1 and 46, the limitation is obvious to Hericourt's invention in light of what he discusses is known in the prior art and because he does not place any limitations on the types of certificates used in his invention. One skilled would have been motivated to modify Hericourt's invention such that said TIO comprises a hash value of a trusted entity certificate for the same reasons given in claims 1 and 46.

Hericourt does not explicitly disclose:

1. Said client connecting to said server to determine whether a new TIO is available (col 8, lines 26-39).
2. Said server sending a new TIO to said client if there is a more recent TIO (col 8, lines 26-39).

However, note that the examiner is considering the response from CA Filter 309 as the TIO. The response comprises at least trust level information for a CA and a certificate of the CA. Hericourt discloses that the CA Filter maintains a list of trusted CA's (paragraphs 135-137), where any CA subject to an attack is removed from the list. Samar discloses a client connecting to a server to determine whether a new list of trusted certificates belonging to CA's is available (col 8, lines 26-39). Samar discloses said server sending the new list to said client if there is a more recent list available (col 8, lines 39-44). In light of these teachings, it would have been obvious to one skilled in the art to further modify Hericourt's invention according to the limitations recited in claim 14. It would have been obvious because the TIO as disclosed by Hericourt comprise information indicating the trust level of a CA and the certificate of the CA. The list disclosed by Samar indicates which certificates are trusted and by extension, which CA's are trusted, thus the list is serving the same functionality as the trust level information sent as a response from the CA Filter in Hericourt's invention. One skilled would have been motivated to incorporate Samar's teachings within Hericourt's invention because it would prevent untrustworthy certificates from CA's that are not

longer trustworthy from accidentally being used. Note this is something Hericourt wants (paragraph 10).

Claim 15:

Hericourt and Samar renders obvious all the limitations recited in claim 14. Further, Samar discloses sending a TIO including a signing certificate to said client, wherein trust information of said signing certificates indicates that said signing certificate can be trusted for signing said TIO (col 3, lines 4-13).

Claim 16:

Hericourt and Samar renders obvious all the limitations recited in claim 14. Samar further discloses wherein said client fetches said TIO from a trusted server, said client ensuring that a root certificate that signed said signing certificate is contained in said TIO (Fig 5).

Samar does not disclose said root certificate is not revocable. However, the examiner asserts that non-revocable certificates were well known in the art at the time applicant's invention was made. It would have been obvious to one of ordinary skill in the art to further modify Hericourt's invention such that the root certificate was not revocable because it would indicate a high level of trust for the user of the root certificate.

Claim 17:

Hericourt and Samar renders obvious all the limitations recited in claim 14. Samar further discloses wherein said client verifies a digital signature of said TIO with a

signing certificate, along with a TIO sent to said client (col 5, lines 46-51 and col 7, lines 17-23).

Claim 20:

Hericourt and Samar renders obvious all the limitations recited in claim 14. Hericourt does not explicitly disclose wherein said TIO is delivered to said client via a broadcast channel; wherein a provider delivers an initial TIO to said client that contains a signing certificate and associated trust information by either of including said signing certificate in the initial TIO saved in a client persistent memory, or by sending the initial TIO to said client through a secure channel before using said broadcast channel.

However, the examiner asserts that the limitation is well known in the art, as discussed in a prior office action. At the time applicant's invention was made, it would have been obvious to one of ordinary skill to further modify Hericourt's invention to use a broadcast channel as recited in claim 20. One skilled would have been motivated to do so because sending a TIO via a broadcast channel is the quickest and cheapest way of distributing the same information to a large group of clients. One of ordinary skill would have been motivated to deliver an initial TIO to the client via a secure channel before using a broadcast channel as this would initially ensure that only authorized clients received subsequent TIO's.

Claim 21:

Hericourt and Samar renders obvious all the limitations recited in claim 14. Hericourt does not explicitly disclose updating said TIO on a per session basis when said TIO is not persistently stored. However, as discussed in the prior office action, this

limitation was well known in the art at the time applicant's invention was made. It would have been obvious to one skilled to have further modified Hericourt's invention according to the limitations recited in claim 21. One skilled would have been motivated to do so because it would prevent untrustworthy certificates from being used.

Claim 38:

Claim 38 is directed towards an apparatus comprising a client device which performs the method of claim 14, thus is rejected for much the same reasons given in claim 14. Note Hericourt discloses a client device which stores the response from CA Filter 309, i.e. the TIO, (Fig 3, item 302 and paragraph 107), thus has memory.

Claims 39-41 and 44-45:

Claims 39-41 and 44-45 recite limitations substantially similar to what is recited in claims 15-17 and 20-21 respectively and are rejected for the same reasons given therein.

Claims 18-19 and 42-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hericourt et al (US 2002/0078347) in view of Samar (US 6,304,974) and further in view of Vogel et al (US 6,816,900).

Claim 18:

Hericourt and Samar renders obvious all the limitations recited in claim 17. Hericourt does not explicitly disclose wherein multiple signatures are verified, depending

on the number of signatures specified in said TIO; wherein said client hashes said signing certificates one by one; and wherein if proper results are found in said TIO and said certificates are trusted for signing said TIO, then said TIO proves that it was not tampered with.

However, Vogel discloses wherein multiple signatures are verified, depending on the number of signatures specified in a TIO (col 8, lines 9-17). Vogel also does not explicitly disclose wherein if proper results are found in said TIO and said certificates are trusted for signing said TIO, then said TIO proves that it was not tampered with. However, the purposes of signatures are to verify and validate. If proper results are found for the signatures, then by definition, the TIO has proven that it was not tampered with.

It would have been obvious to one of ordinary skill to further modify Hericourt's invention according to the limitation recited in claim 18 in light of Vogel's teachings because it would allow one to determine which CA's are no longer trustworthy due to possible security breaches. Note Hericourt discloses wanting to remove untrustworthy CA's from the list of trusted CA's (paragraphs 136-137).

Claim 19:

Hericourt and Samar renders obvious all the limitations recited in claim 19. Hericourt does not explicitly disclose wherein said signing certificates exist in said TIO in said client before said TIO is signed. However, official notice is taken that at the time applicant's invention was made, it was well known for a client to receive and store a signing certificate from a CA before messages signed with the certificate is sent to the

client. In light of this, it would have been obvious for one skilled to have further modify Hericourt's invention according to the limitations recited in claim 19. One skilled would have been motivated to do so because it would allow a client to quickly verify the authenticity of a message/response/TIO received if the client already had the signing certificate with which it can perform authentication of a signature.

Claims 42-43:

Claims 42-43 recite limitations substantially similar to what is recited in claims 18-19 respectively and are rejected for much the same reasons. The most noticeable difference between claim 42 and 18 is that claim 42 recites said client device utilizes said TIO. This limitation is also disclosed b Hericourt (paragraph 111).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Ponnoreay Pich
Examiner
Art Unit 2135

PP

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100